GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (*pro hac vice*)
lgoldman@gibsondunn.com
DARCY C. HARRIS (*pro hac vice*)
dharris@gibsondunn.com
200 Park Avenue
New York, NY 10166-0193
Telephone: (212) 351-4000
Facsimile: (212) 351-4035

ELIZABETH K. MCCLOSKEY, SBN 268184
emccloskey@gibsondunn.com
ABIGAIL A. BARRERA, SBN 301746
abarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

Attorneys for Defendant Meta Platforms, Inc.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ALAN STARZINSKI, et al.,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:24-cv-04501-AMO

DEFENDANT META PLATFORMS, INC.'S REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED CLASS ACTION COMPLAINT

Date: June 26, 2025
Time: 2:00 p.m.
Dept.: Courtroom 10 – 19th Flr.

Action Filed: June 27, 2024
Honorable Araceli Martínez-Olguín

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Despite amending their complaint in response to Meta's prior motion to dismiss, plaintiffs still fail to state any claim against Meta based on third-party streaming services' alleged misuse of a publicly available, widely used internet tool. Across the board, plaintiffs' opposition brief fails to show otherwise; instead, plaintiffs repeatedly ask this Court to lower the bar in ways inconsistent with binding Ninth Circuit precedent. The Court should reject that invitation and dismiss the complaint.

The most glaring problem with plaintiffs' claims is their failure to plausibly allege that Meta *intended* for the streaming services to misuse the Meta Pixel by sending data in violation of the streaming services' express agreements with Meta. Judge Chhabria analyzed the same issue under controlling Ninth Circuit precedent in *Doe I v. Google LLC*, 741 F. Supp. 3d 828 (N.D. Cal. 2024) ("*Google Pixel*"), and dismissed materially identical allegations as insufficient. Plaintiffs ask the Court to reject Judge Chhabria's analysis and adopt a lower standard for intent, but there is no sound basis to do so.

Plaintiffs' claims independently fail because they consented to Meta's receipt of their data, both when they agreed to the streaming services' privacy policies and when they agreed to Meta's. For the streaming services' policies, plaintiffs try to kick the can down the road by suggesting that maybe somehow the sign-up flows or policies were different when they signed up for their accounts—even though plaintiffs *affirmatively invoke* their relationship with the streaming services (specifically, their subscriber status) to make out *other* parts of their claims, and never argue or allege that they did not agree to the streaming services' terms when they signed up. For Meta's policies, plaintiffs ask for a special, heightened standard for consent: listing out in advance each specific type of data third-party websites might choose to send. But that is irreconcilable with binding Ninth Circuit precedent and would be impossible to implement in practice. This Court should reject those arguments.

Nor do plaintiffs plug other claim-specific gaps. The federal Wiretap Act's one-party consent rule forecloses that claim, regardless of whether plaintiffs also consented. Plaintiffs' suggestion that URLs are "content" whenever they contain video titles contravenes Ninth Circuit precedent. And plaintiffs wholly fail to allege the outrageous, highly offensive conduct needed to state a privacy tort.

Because these problems persist even after amendment, this Court should dismiss with prejudice.

ARGUMENT

Whatever claims plaintiffs might have against the streaming services that allegedly chose to share the information at issue, it is clear they have none against Meta merely for receiving it. This Court should dismiss the complaint with prejudice.

I. Plaintiffs Do Not Allege Meta Intended To Intercept Their Sensitive Data.

Plaintiffs concede (at 7) that, to plausibly allege intent, they had to plead facts showing that Meta "purposefully and deliberately" intercepted their allegedly sensitive video-viewing data. *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015) (quotation marks omitted); *see also id.* at 775 ("conscious objective") (quotation marks omitted). Yet even after amending their complaint, plaintiffs did not do that. Rather, the amended complaint reiterates that Meta *forbade* third parties, including the streaming services here, from sending any such information. Mot. 8–13. That failure is fatal: as Judge Chhabria explained in another pixel case, "[i]f a plaintiff alleges that the clients of a source code provider use the code contrary to the provider's instructions, the plaintiff should not be able to get around the intent requirement by simply intoning that the source code provider intended for the clients not to follow instructions." *Google Pixel*, 741 F. Supp. 3d at 841; *accord B.K. v. Desert Care Network*, 2024 WL 1343305, at *7 (C.D. Cal. Feb. 1, 2024) (finding no intent by Meta).

Plaintiffs make two basic arguments in response. First, they ask this Court to reject Judge Chhabria's analysis and adopt a lower standard for alleging intent. Second, they halfheartedly try to distinguish the allegations in this case from those in the *Google Pixel* case. Neither argument holds up: Judge Chhabria's analysis is correct under binding Ninth Circuit precedent, and application of that standard clearly dictates dismissal.

A. The Ninth Circuit's *Christensen* Standard Requires A Conscious Objective, Not Mere Awareness.

As Meta's motion acknowledged (at 12), there is an intra-District split over the meaning of "intent." Some courts have held that "interceptions may be considered intentional where a defendant is aware of the defect causing interception and takes no remedial action." *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020). Plaintiffs rely on that standard and several cases applying it, and they maintain that they "have adequately alleged both [Meta's] knowledge of the

unlawful interception and its failure to take remedial action." Opp. 13.[1] But as Judge Chhabria held in *Google Pixel*, that "is not the right way to think about intent" and "set[s] the legal bar too low." 741 F. Supp. 3d at 840. And as Meta showed, plaintiffs' allegations of intent plainly fail under the standard Judge Chhabria applied. Mot. 8–13. For several reasons, this Court should apply that standard here and reject plaintiffs' request to lower the bar.

First, the "awareness" standard is inconsistent with binding Ninth Circuit precedent. In *Christensen*, as plaintiffs recognize (at 7), the Ninth Circuit made clear that "intentionally" means "purposefully and deliberately," with the "conscious objective" of intercepting the communications at issue. 828 F.3d at 774–75. That "suggests something more than mere awareness that an interception might occur due to the failure of [the streaming services] to follow instructions." *Google Pixel*, 741 F. Supp. 3d at 840. In short, a party can be *aware* that something is happening without having any *conscious objective* to bring about that result.

Second, to the extent an awareness standard is ever appropriate, it should not apply in cases (like this one) alleging third-party misconduct. In early cases applying the awareness standard, the defendant was wholly responsible for an alleged "defect" in its own product that resulted in interceptions, and the courts inferred intent based on the defendant's failure to fix that defect. *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 815 (voice-activated Google Assistant software recorded conversations even when no one said a "hotword" to activate it); *see also, e.g.*, *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021) (same, for Apple's Siri software); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) (Apple's iMessage software intercepted text messages from former users). In those cases, it was the combination of the defendant's knowledge, sole control over the defective product, and failure to take action that enabled the courts to infer intent. *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 815 (defendant knew a defect in its own product "cause[d]

[1] One of the cases plaintiffs rely on (at 9), *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041 (N.D. Cal. Dec. 30, 2024), is entirely inapposite. That case involved video-viewing data from public news and home-improvement websites, not streaming services, and there was no plausible allegation that disclosing that data violated the VPPA. *See, e.g.*, *Carroll v. Chick-fil-A, Inc.*, 2024 WL 1091193, at *2 (N.D. Cal. Feb. 13, 2024) ("publicly available, free videos on a website" do not implicate the VPPA). Because the data in *Yoon* did not even arguably implicate the VPPA, Meta did not raise, and the court did not address, the intent issue presented here.

[recordings] to be made, yet ha[d] not fixed the problem"); *Lopez*, 519 F. Supp. 3d at 684 (similar, and noting "the question is close"); *Backhaut*, 74 F. Supp. 3d at 1044 (similar). But here, there is no "defect" in the Meta Pixel for Meta to "remediate." Nor did Meta retain sole control over how the streaming services configured the Pixel, a publicly available and widely used tool that each web developer can customize for its own purposes. Rather, this is a case alleging third-party misconduct: plaintiffs allege *the streaming services* "knowingly" used the Pixel improperly to "violate the Video Privacy Protection Act." Compl. ¶ 80. And it is not plausible to infer intent from the failure to prevent third-party misconduct. *See Google Pixel*, 741 F. Supp. 3d at 840 (rejecting argument that "Google is capable of preventing the inadvertent transmission of private information from health care provider websites, and that its failure to do so is reflective of an intent to obtain the information").

Third, plaintiffs' watered-down theory of intent would effectively render the intent requirement meaningless. Pixel technology is widely used by millions of web developers spanning countless industries, each with their own regulatory frameworks and rules for "sensitive" information. The entities in those industries—whether hospitals, video-streaming services, or any others—are responsible for complying with those rules. But as the recent proliferation of pixel-related litigation across the country confirms, plaintiffs' theory would expose source-code providers like Meta and Google to litigation every time a third party allegedly misuses pixel technology on its own website.

As Judge Chhabria correctly concluded, plaintiffs' theory of intent is flawed and contrary to Ninth Circuit precedent. This Court should reject it.

B. Plaintiffs Cannot Satisfy The *Christensen* Standard.

Plaintiffs halfheartedly argue that their allegations could satisfy the higher *Christensen* standard, deeming Judge Chhabria's analysis in *Google Pixel* "distinguishable." Opp. 11. That argument falls flat.

First, plaintiffs say that they "allege [Meta] closely consulted with the Streaming Services in integrating the Business Tools and knew from that close contact that it was receiving confidential information." Opp. 11. That fails several times over. For one thing, even on its own terms, it merely reflects *awareness*—not *intent*—and thus still fails under the proper legal standard. *See supra* 2–4. For another, it is no distinction of *Google Pixel*, where the plaintiffs alleged more—that Google

"*encourage[d]*" healthcare providers to use its pixel tool to send protected health information—to no avail. *Google Pixel*, Dkt. 86 ¶ 306, No. 3:23-cv-2431 (N.D. Cal. Nov. 16, 2023) (complaint) (emphasis added); *see also, e.g.*, *id.* ¶¶ 440, 511, 540 (alleging Google "conspired with Health Care Providers" and "provid[ed] instructions to Health Care Providers" on how to use the Google Pixel). And, finally, plaintiffs' vague and conclusory factual allegations do not show that Meta instructed the streaming services to configure the Pixel in a way that would send sensitive data in violation of Meta's policies. Meta's motion pointed out these factual gaps (at 12–13), and plaintiffs' opposition brief offers no meaningful response; instead, plaintiffs simply fall back (at 13) to the improper "awareness" standard.

Second, plaintiffs say that Meta "knowingly receives the confidential video-viewing information and integrates it into its proprietary advertising products." Opp. 12. But the same problems repeat themselves. Again, even on its own terms, this merely asserts *awareness* that information is entering Meta's automated systems (and not even awareness that the information was shared without consent), not a "conscious objective" to receive sensitive information without consent. *Christensen*, 828 F.3d at 775 (quotation marks omitted); *see supra* 2–4. Again, plaintiffs are wrong to suggest the allegations were any different in *Google Pixel*. *See, e.g.*, Dkt. 86 ¶¶ 7, 105, 123, 224, 408–09, No. 3:23-cv-2431 (alleging "Google uses the information for marketing in its advertising systems and products," and that "Google's conduct is knowing and intentional" because "collection permits Google to obtain significant profits"). And again, plaintiffs' generalized allegations about how pixel technology operates—*i.e.*, that the Pixel is designed to collect data from third-party websites, and that Pixel data enters Meta's automated systems and is used for advertising purposes—does not show any specific intent to acquire and use *sensitive* data sent in violation of Meta's policies.

At bottom, plaintiffs' allegations establish, at most, third-party misuse (by the streaming services) of a free, publicly available, and common internet tool, contrary to Meta's policies against sending sensitive data. Whatever claims those allegations might give plaintiffs against the streaming services, plaintiffs have not alleged any facts showing that *Meta intended* this alleged misuse. As Judge Chhabria concluded in *Google Pixel*, that requires dismissal.

II. Plaintiffs Consented To Meta's Receipt Of Their Data.

Plaintiffs' claims also fail because they agreed to policies disclosing the precise conduct of

which they now complain—both the streaming services' policies, and Meta's. Mot. 13–20. Plaintiffs cannot bring claims based on data-sharing they agreed to when they signed up for streaming and Facebook accounts, and here again, their responses do not withstand examination. Although plaintiffs argue (at 13) that Meta bears the burden to show consent, lack of consent is an *element* of several of plaintiffs' claims that they must plead to state a claim. *See* Mot. 13–14. Regardless, "it does not matter, because in either case the question is whether the allegations in the complaint and any judicially noticeable materials definitively establish that the plaintiffs consented to the conduct." *Rickwalder v. Meta Platforms, Inc.*, 2022 WL 22462351, at *10 n.5 (Cal. Super. Ct. Sept. 15, 2022) (quotation marks omitted). "If the answer is yes, the Court must dismiss the claims regardless of whether consent is an element or a defense." *Id.*

A. The Streaming Services' Policies Establish Plaintiffs' Consent.

All four streaming services—Paramount+, Hulu, ESPN+, and Starz—explicitly disclosed to users (including plaintiffs) that they would share data with social media companies, like Meta, about users' activities on their platforms. Mot. 4–5, 16. Those disclosures, which plaintiffs agreed to when they allegedly became subscribers, establish plaintiffs' consent. *See id.* at 14–15.

Tellingly, plaintiffs' leading response is a procedural dodge. Plaintiffs say that, at the motion-to-dismiss stage, the Court cannot infer from the *current* versions of the streaming services' sign-up pages and privacy policies that the same sign-up processes or disclosures existed in the past. Opp. 13–14. Those arguments are makeweights: plaintiffs do not actually contend there are any relevant differences in prior versions of the sign-up pages or the privacy policies, nor do they allege that they somehow signed up for streaming-service accounts without agreeing to the streaming services' terms. Plaintiffs simply seek to skate past a motion to dismiss without having to deal with the streaming services' disclosures. That is pure gamesmanship, especially given plaintiffs' selective reliance on their subscriber status to make out *other* parts of their claims—namely, that the VPPA protects the data at issue (the core of plaintiffs' claim that this data is "sensitive"). *See, e.g.*, Compl. ¶¶ 1, 23–26, 47, 80–81 (alleging plaintiffs are "subscribers and therefore consumers" under the VPPA). In any event, this is an issue that could quickly be resolved. If the only things standing in the way of dismissal are the issues of whether plaintiffs agreed to the streaming services' policies when they became subscribers

and whether those policies have contained materially similar disclosures over time, then this Court should order targeted discovery to resolve those issues and bring a quick end to this case via summary judgment. *Cf. In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1164–67 (N.D. Cal. 2016) (finding assent after evidentiary hearing). There is no good reason for the parties and the Court to go through years of litigation when the streaming services' policies clearly establish consent.

On the merits, plaintiffs have very little to say. They assert without analysis that the streaming services' policies "did not 'explicitly notify' [them] of the practice at issue." Opp. 14–15 (quoting *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021)). But that is simply wrong, and plaintiffs never engage with the explicit language from the streaming services' policies—including express disclosures that the streaming services "share your personal information" with "social media companies such as Meta," such as "browsing habits," "content choices," "the content you view," "title selections," and "shows you have watched." Mot. 4–5, 16 (collecting relevant language).

Plaintiffs also suggest the streaming services' privacy policies cannot establish consent because the VPPA requires "a form distinct and separate from any form setting forth other legal or financial obligations." 18 U.S.C. § 2710(b)(2)(B)(i); *see* Opp. 15. But that is legally irrelevant. Plaintiffs have not asserted (and could not assert) any freestanding VPPA claim against Meta. Instead, they have asserted wiretapping and privacy claims, where privacy policies with on-point disclosures are sufficient to establish consent. Mot. 14–15, 16–17 (collecting cases). Plaintiffs cite no authority for the proposition that the VPPA's disclosure requirements may be imported into their wiretapping or privacy claims. Indeed, plaintiffs' VPPA argument only confirms that they have sued the wrong party: if they want to assert a VPPA claim for wrongful disclosure of their data, the proper defendants are the streaming services, not Meta. *See* 18 U.S.C. § 2710(b)(1), (c) (providing a private right of action against "*a video tape service provider* who knowingly *discloses*" video-viewing information, not against entities that merely *receive* that information) (emphases added).

B. Meta's Policies Establish Plaintiffs' Consent.

Meta's policies likewise disclosed to Facebook users (including plaintiffs) that Meta could receive data from third-party websites, like the streaming services here, reflecting users' activity on those sites. Mot. 5–7, 17–18. Those disclosures, too, establish consent, and plaintiffs' arguments to the

contrary fail to account for what Meta's policies actually say.

Plaintiffs admit (indeed, affirmatively allege) that Facebook users like themselves "assent[] to" Meta's policies. Compl. ¶ 89. And they do not contest that other cases, including from the Ninth Circuit, have held that Meta's policies establish consent for Meta to receive data reflecting Facebook users' activity on third-party websites. *See, e.g.*, *Lloyd v. Facebook, Inc.*, 2024 WL 3325389, at *2 (9th Cir. July 8, 2024) (affirming dismissal of privacy claims because "Facebook's data policy gives clear notice that third party partners may share data with Facebook"); *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8–9 (9th Cir. 2018) (similar, for "browsing data from various healthcare-related websites"). That should be the ballgame.

Echoing recent district court decisions in the health- and financial-data contexts, plaintiffs nonetheless insist that where allegedly "sensitive" data is at issue, "the defendant must provide *specific notice of the precise type of sensitive information* disclosed." Opp. 15–16 (emphasis added); *see also id.* at 18 (asking for a "heightened requirement of a specific disclosure"). That "heightened requirement" is impossible to square with Ninth Circuit caselaw. When the Ninth Circuit in *Smith* affirmed dismissal of claims concerning "browsing data from various healthcare-related websites," it never asked whether Meta specifically identified health-related data in its disclosures; instead, the court concluded that "many other kinds of information are equally sensitive," and that "the practice complained of falls within the scope of [p]laintiffs' consent to Facebook's Terms and Policies." 745 F. App'x at 8–9. Similarly, in *Hammerling v. Google, LLC*, the Ninth Circuit recently reiterated that courts must give full effect to broad disclosures that "Google collects activity data in third-party apps downloaded to Android devices," even if the breadth of the disclosures arguably "deviate[s] from our expectations" in particular instances. 2024 WL 937247, at *1–2 (9th Cir. Mar. 5, 2024).[2] These decisions illustrate the principle that "[a] contractual term is not ambiguous just because it is broad." *F.B.T. Prods., LLC*

[2] Plaintiffs argue that "the Ninth Circuit distinguished *Hammerling* in *Calhoun*," Opp. 18, but that distinction has nothing to do with *Hammerling*'s relevance to this case. In *Calhoun*, the parties disputed which of several privacy policies governed the data collection at issue, and the court noted that there was no such dispute in *Hammerling* (or in *Smith*). *See* 113 F.4th 1141, 1149 (9th Cir. 2024). There is no such dispute here, either: as in *Hammerling* (and *Smith*), everyone agrees that the relevant user-facing policies are Meta's Terms of Service, Privacy Policy (previously called the Data Policy), and Cookies Policy. *See* Compl. ¶ 89; Mot. 17; Opp. 16. The question here, as in *Hammerling* and *Smith*, is the scope of consent established by those policies.

v. Aftermath Recs., 621 F.3d 958, 964 (9th Cir. 2010). And Meta's broad disclosures "explicitly notify users of the conduct at issue" by alerting users that third-party websites can share data with Meta reflecting users' activity. *Calhoun*, 113 F.4th at 1147 (quotation marks omitted); *see also* Mot. 5–6 (collecting relevant disclosures).

Plaintiffs' proposed "heightened requirement" for disclosures of "sensitive" data, Opp. 18, is therefore baseless. That purported requirement would also be wildly impracticable, given that any web developer in any industry can use the Meta Pixel and choose what kind of data they want to send; Meta could not possibly list out in advance every kind of data third parties might choose to send.

Plaintiffs also note that Meta's Privacy Policy states that Meta requires third-party websites (like the streaming services) to have the right to share any data they choose to share. Opp. 16 (citing Compl. ¶¶ 88, 92). That statement in the Privacy Policy is true, and it does nothing to limit the scope of plaintiffs' consent. As plaintiffs acknowledge, Meta *does* contractually require every party who uses the Business Tools to have "all of the necessary rights and permissions . . . for the disclosure and use of Business Tool Data." Ex. 4. Meta specifically forbids those parties from sending any "sensitive information," including "any information defined as sensitive under applicable laws," through the Business Tools. *Id.*; *see also* Opp. 17 (acknowledging this provision). Those contractual restrictions on third-party conduct do not limit the scope of consent established by Meta's agreements with Facebook users. To the contrary, it is perfectly acceptable for Meta to obtain a broad scope of consent from users and then place narrower restrictions on third-party websites—and those websites' alleged failure to comply with Meta's restrictions does not change the scope of users' consent.

Similarly, plaintiffs are wrong to say that Meta "violated its own terms" by allegedly receiving their data from the streaming services. Opp. 16 (citing Meta's Business Tools Terms). It is *the streaming services* that allegedly violated their commitments to *Meta*, embodied in Meta's Business Tools Terms (to which plaintiffs are not parties), by sending any information they lacked the legal right to send or that was otherwise purportedly sensitive. And, again, that alleged third-party violation does not somehow vitiate or limit the scope of plaintiffs' consent as set out in their own agreements with Meta.

III. Plaintiffs' Claims Also Fail For Other Claim-Specific Reasons.

In addition to intent and consent, plaintiffs also failed to plead multiple other essential elements of their claims. Mot. 20–25. These failures are independently fatal, and plaintiffs' opposition brief does not cure them.

A. Web Developers' Consent Defeats Plaintiffs' Federal Wiretapping Claim.

The federal Wiretap Act does not apply if even *one* party to a communication consented to share it. 18 U.S.C. § 2511(2)(d). Here, even putting aside plaintiffs' consent, the complaint affirmatively and repeatedly alleges that the streaming services knowingly chose to share the data at issue with Meta. Mot. 20–21. That means Meta cannot be liable.

Plaintiffs do not contest that the streaming services consented to share information with Meta. Instead, they argue that this consent is invalid under the crime-tort exception. *See* 18 U.S.C. § 2511(2)(d) (one-party consent precludes liability "unless such communication is intercepted for the purpose of committing any criminal or tortious act"); Opp. 20–22. Relying chiefly on *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021), plaintiffs argue that "the surreptitious tracking of users on the internet falls under this exception." Opp. 21. But even putting aside plaintiffs' incorrect assumption that the tracking here is surreptitious, that argument improperly focuses on "whether *the interception itself* violated another law"—an argument the Ninth Circuit has expressly rejected. *Sussman v. Am. Broad. Cos.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (emphasis added; quotation marks omitted). As the Ninth Circuit recently emphasized (in a case decided after *Brown*), to qualify for the crime-tort exception, the "criminal or tortious purpose must be *separate and independent* from the act of the recording"—for example, where a person unlawfully records someone intending to "facilitat[e] some further impropriety, such as blackmail." *Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1135–36 (9th Cir. 2022) (emphasis added; quotation marks omitted). As numerous cases have held, using web-browsing data for advertising purposes is not separately and independently criminal or tortious (unlike blackmail); to the contrary, that commonplace activity is perfectly lawful. *See, e.g.*, *Google Pixel*, 741 F. Supp. 3d at 843 n.4 (rejecting crime-tort argument); *see also* Mot. 22 & n.5 (collecting cases). Plaintiffs' argument that it becomes criminal or tortious merely because the interception itself was allegedly unlawful employs the same circular reasoning the Ninth Circuit rejected in

Newman. *See* 51 F.4th at 1136 ("§ 2511(2)(d) requires that the criminal or tortious purpose be independent of and separate from the purpose of the recording. Planned Parenthood runs afoul of this requirement by reusing the same criminal purpose . . . as both the purpose of the civil RICO claim and the independent criminal or tortious purpose of § 2511(2)(d).").

B. Plaintiffs Fail To Allege Meta Received The "Contents" Of Any Communication.

Plaintiffs' claims under the federal Wiretap Act and CIPA § 631 are limited to the "contents" of communications—*i.e.*, the intended message conveyed (like the text of an online chat or the answers typed into a questionnaire), rather than data merely reflecting *actions* taken on a website (like viewing a webpage or clicking a button). Mot. 23–24. Plaintiffs do not allege Meta received any such information, so their claims must be dismissed. *See id.*

Plaintiffs assert that "video-specific URLs" are contents. Opp. 22. That is simply wrong. As the Ninth Circuit has explained, "the webpage address identifies the location of a webpage a user is viewing on the internet" and is not "contents." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014). That is true even when the URL reveals arguably sensitive information. *See id.* at 1108 (rejecting argument that URL constituted contents where it revealed a user "was viewing the Facebook page of a gay support group"). Indeed, in a similar case alleging interception of video-viewing information—which Meta cited in its motion, and plaintiffs simply ignore—a court rejected the precise argument plaintiffs assert here and held that "the file path and video title information contained in the URLs allegedly intercepted" were not "content." *In re Nickelodeon Consumer Priv. Litig.*, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) (dismissing wiretapping claim).

The cases plaintiffs cite (at 22–23) are not to the contrary. Rather, those cases stand for the proposition that the *search terms* a user types into a search bar (which may sometimes be *revealed* in a URL) may qualify as contents. *See Cousin v. Sharp Healthcare*, 702 F. Supp. 3d 967, 976 (S.D. Cal. 2023) ("data included personal search queries"); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1051–52 (S.D. Cal. 2023) (data included "search terms"); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022) ("the transmitted URLs include both the 'path' and the 'query string'"); *Hammerling v. Google LLC*, 2022 WL 17365255, at *10 (N.D. Cal. Dec. 1, 2022) (data included "products [users] searched for"). That proposition is consistent with the Ninth Circuit's

recognition that "[u]nder some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL *containing that search term* to a third party could amount to disclosure of the contents of a communication." *Zynga*, 750 F.3d at 1108–09 (emphasis added). But a URL that merely reflects which webpages a user visited is not contents, even if that URL includes the title of the video hosted on that webpage. *See id.* at 1107–08; *accord In re Nickelodeon*, 2014 WL 3012873, at *15.

C. Plaintiffs Fail To Allege Any "Highly Offensive" Conduct.

Plaintiffs' privacy torts, a new addition in their amended complaint, require them to plead more than a simple privacy intrusion; plaintiffs must plead that any such intrusion was an egregious, highly offensive breach of social norms, the sort of conduct that sparks a reasonable person to outrage. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009). Tracking users' online web browsing does not clear that high bar. Mot. 24–25.

Plaintiffs offer no response at all to *Hubbard v. Google LLC*, 2024 WL 3302066 (N.D. Cal. July 1, 2024). That case involved Google's alleged collection of children's video-viewing data on YouTube without consent, allegedly in violation of the Children's Online Privacy Protection Act. *See id.* at *1–2. The court extensively analyzed the "highly offensive" element, concluded it was not satisfied, and dismissed the plaintiffs' privacy claims. *Id.* at *6–8. The same result is warranted here *a fortiori*, where children's data is not at issue and Meta is merely the *recipient* of data that plaintiffs allege the streaming services sent.

Plaintiffs suggest (at 24) this element is incapable of resolution at the pleading stage. Not so: courts "do in fact[] decide the 'highly offensive' issue as a matter of law at the pleading stage when appropriate." *Hubbard*, 2024 WL 3302066, at *7 (quoting *Boring v. Google Inc.*, 362 F. App'x 273, 279 (3d Cir. 2010)); *see also* Mot. 24–25 (collecting cases). Plaintiffs also suggest (at 24) their claim should survive because they allege Meta "surreptitiously" collected their data. But "[e]ven assuming this information was transmitted without [p]laintiffs' knowledge and consent, a fact disputed by [Meta], such disclosure does not constitute an egregious breach of social norms." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012). The same goes for plaintiffs' argument (at 25) that their data is protected under the VPPA and similar state statutes: "violations of law do not

necessarily represent highly offensive behavior." *Hubbard*, 2024 WL 3302066, at *8 (dismissing privacy claims despite allegations that defendant violated Children's Online Privacy Protection Act). Plaintiffs ultimately fall back to cases against Meta alleging collection of protected health information. Opp. 24–25. Meta respectfully submits those cases were wrongly decided, but even taking them as a given, they focused on the peculiar nature and treatment of "protected health information." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 800; *see also id.* at 799 ("[H]ealth-related communications with a medical provider are almost uniquely personal."); *see also E.H. v. Meta Platforms, Inc.*, 2024 WL 557728, at *2–3 (N.D. Cal. Feb. 12, 2024) (similarly alleging collection of protected health information); *Doe v. FullStory, Inc.*, 712 F. Supp. 3d 1244, 1257 (N.D. Cal. 2024) (same). Their analysis pertained to "the kind of information at issue [t]here," *see In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 801, and does not support plaintiffs' attempted expansion to a new context—particularly where cases dealing with video-viewing data (like *Hubbard*) have since come out differently.

Privacy claims set a "high bar." *Belluomini v. Citigroup Inc.*, 2013 WL 5645168, at *3 (N.D. Cal. Oct. 16, 2013). They are reserved for egregious, highly offensive conduct, and not every claim of improper online data collection (even assuming that is what happened here) will meet that standard. Here, as in *Hubbard*, plaintiffs' allegations fall far short.

CONCLUSION

The Court should dismiss the complaint with prejudice.

DATED: February 18, 2025

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Lauren R. Goldman*
Lauren R. Goldman